Many of the procedures associated with limited use cards represent functions already performed by the clearing systems. These existing functions include: adding new credit/debit card numbers to the processing databases; allowing these card numbers to be activated following a confirmatory call to the issuer by the customer; conferring a credit limit on a credit card number; and invalidating a credit card number from further use and marking any further use as fraudulent. This overlap represents part of the commercial value of the single use invention, minimizing the required changes.

Once a limited use number enters the clearing system it can be handled in a normal fashion, e.g., by ensuring that it has not been reported as being stolen and that it represents a valid account number within the database. If the transaction is within the credit limit of the customer and the transaction limit or restricted use limitations of the limited use number, it is authorized.

Several specific modifications should be made to the processing software to implement the features of limited use cards. For instance, valid limited use numbers are stored in a database of valid account numbers along with other information specific to limited use numbers. This includes sufficient information to identify the customer to whom it was issued and any additional limitations placed upon the card in terms of transaction value or category of merchant for which the card can be used.

Once authorized, the limited use number is invalidated so as to ensure that further authorization/charges cannot be made on that number. To allow for authorization preceding request for settlement by a substantial delay, for example in the context of a mail order purchase where a credit/debit card number may be authorized at the time of order and charged only when the product ships, delayed settlement to the same merchant must be allowed.

Once the number of transactions permitted for a limited use card is reached, the central card processing software invalidates the card. Due to the time delay that can occur between authorization and a merchant request for settlement, improved security

is achieved by linking the invalidation process to authorization. Linking invalidation to settlement facilitates pre-authorizations at the cost of increased risk of, for example, multiple use of a card number intended for limited use. Pre-authorizations can be used with authorization dependent invalidation as described above. In the case where a transaction is not authorized before being accepted by a merchant, the invalidation process will occur when the transaction details are transmitted to the processor for settlement. When no authorization is obtained for a limited use number the system will therefore still operate normally with an increased level of risk for the issuer/merchant as is the case with an unauthorized conventional card transaction.

Whenever the credit limit or validity of a customer's account changes, all currently valid limited use numbers are identified and their associated credit limit is altered to the lower of either their allocated transaction or the existing credit limit. If the customer account is closed or declared delinquent, all valid single use numbers are handled in the same manner.

Whenever a limited use number is used, the next available single use number previously allocated to the same customer and issued to the customer is added to the database of valid account numbers.

When a transaction is charged to a limited use number, the transaction details and customer account details are stored together for audit purposes and the value of the transaction is added to the customer's account for billing.

The software for storing transaction details and printing statements can be modified to allow for both the customer's conventional account details and the limited use number transaction details to be reported.

Processing of limited use numbers can be integrated into existing systems in a variety of ways. The authorization and settlement process can be completed in a single cycle or split into a separate authorization and settlement processes as is commonly done in existing credit card systems.

In the case of an entirely new, stand-alone, limited use credit/debit/charge card processing system, the above functions can be implemented without restriction in any suitable computer capable of incorporating the required database and communication functions. Such a system should be able to provide an authorization for a transaction within the same time scale as an existing credit/debit/charge card transaction.

In the case where the above functions have to be integrated into existing systems several approaches can be taken to minimize the required changes. It is possible to add steps to the processing chain that is encountered as soon as a credit/debit/charge card number is received from a merchant.

Fig. 7 is a flow chart illustrating an exemplary process for processing a transaction. In step 702, a software system receives transaction details from a merchant. The software system determines whether the number is a limited use number or a conventional card number. (Step 704). If the number is a conventional card number, it is passed on unchanged into the processing system and can be handled by existing systems with no modification. (Step 706). The merchant receives authorization from the system responsible for authorizing conventional card numbers. Merchant reimbursement is similarly unaffected. (Step 708).

The system can check the limited use number and the corresponding limitations. (Step 710). If the number is not valid for the designated transaction, the transaction is denied. (Step 712). Otherwise, a database look-up procedure determines the associated master account number and transmits this number (i.e. the master account number) back into the processing system. (Step 714). This allows all existing fraud detection, authorization and demographic software procedures to be completed with no alteration. (Step 716). Once the master account number is substituted for the limited use number a number of additional steps are required. (Step 718). If the criteria for invalidating the limited use number have been met during this transaction, then the limited use number is invalidated for all future transactions except refunds. An additional limited use number can be automatically issued if a continual supply of

single use numbers is required. The transaction details and master account number are then transmitted for inclusion within a database to allow for tracking of transaction details and billing of the user. These functions do not need to be performed before an authorization is issued but can completed afterwards. (Step 720). However, performing such steps together with the validity verification of the limited use number prior to issuing an authorization message to a merchant is a feasible option with a minor reduction on the processing time required to issue an authorization message.

With the above system, the software responsible for substituting the master account number for the limited use number can also process additional features unique to limited use numbers. These features include transaction value limitations, merchant type restrictions and geographical limitations. If the transaction exceeds the limitations placed on the limited use card then authorization is denied and the master credit card need not be passed on for further processing. In the case of a transaction falling within the limitations of a limited use card, then the transaction details are passed on with the master account number for conventional validation. In this way the restrictions in place for the master account (e.g., available balance, expiry date) are checked for each limited use transaction.

Specific fraud detection mechanisms can also be incorporated into the software. For example, on the first occasion that an invalidated limited use number is used this transaction can be flagged as potentially fraudulent and appropriate measures taken. Repeated attempts to authorize invalid numbers from a single merchant or group of merchants also potentially points to fraud and can lead to activation of appropriate fraud management measures.

The above system requires the least modification of existing systems but may take up to twice the processing time of a conventional transaction due to the double authorization process, once within the limited use verification and translation step and once within the standard systems. It may be advantageous to initially process the limited use card as a master credit card by using a single list of limited use numbers and master credit card numbers.

Fig. 8 is a flow chart illustrating another exemplary process for processing a transaction. In step 802, a software system receives transaction details from a merchant. The software system has access to a database that contains additional information to identify the associated account or means of settlement and specific limitations relating to the use of limited use cards. As a result, limited use numbers can be associated with existing accounts in the manner currently used to associate multiple conventional accounts in the case of multiple cards issued to a single company for corporate use. (Step 804). During an authorization the associated account number need not be identified provided each limited use account is updated whenever the status of the associated account changes (e.g. available balance, account validity etc.). The system can deny authorization (step 806) or authorize a transaction (step 808) without identifying the associated account number.

For settlement and billing purposes (step 812), the associated account needs to be identified (step 810), but this does not need to be done during the course of an authorization. The existing software should be modified or linked to a new program that performs duties specific for limited use card numbers as described above. (Steps 814, 816, and 818). These functions do not need to be performed before an authorization is issued. These functions can be completed afterwards.

This system requires more modification of the existing processing software systems, but offers authorization times within the same timescale as existing transactions since only one authorization steps is involved. Other activities such as updating the limitations on the limited use card when the master account changes can be performed outside the authorization process (i.e., "off-line").

Such other activities can also take place while the system is operating. The system may include some or all of the following features:

1) A system capable of altering the nature and value of limitations associated with a specific limited use credit/debit/charge card number on the basis of the

usage of that specific limited use card number in transactions, where such alteration is conducted while the system is operational;

2) A system capable of altering the nature and value of limitations associated with a specific limited use credit/debit/charge card number on the basis of instructions generating on behalf of the issuing bank, where such alteration is conducted while the system is operational; and

3) A system capable of altering the nature and value of limitation associated with a specific limited use credit/debit/charge card number on the basis of instructions generated on behalf of the card holder, where such alteration is conducted while the system is operational.

The invention is not limited to the embodiments hereinbefore described but may be varied in both construction and detail. For instance, the invention has been heretofore described mainly in the context of a system in which a customer receiving a single use card already has a main account with the credit card provider. But this need not be so. For example, it is envisaged that an ATM machine (or similar apparatus) could be used by people who did not have a credit card account to purchase disposable credit cards, which disposable credit cards could then be used for either card present or remote transactions. When the card had been used, the card would be simply reinserted into the ATM machine, and after a suitable period of time the purchaser's account would be credited with any money not spent. Similarly, if the person who purchases the disposable credit card does not have an account of any sort with the credit card provider, the credit card could still be purchased from the ATM machine and then any refund could take place a sufficient time after the transaction would have been cleared, which refund could be either in the form of a cash refund to the purchaser or to a crediting of that purchaser account with another financial institution. Similarly, it will be appreciated that the use of an ATM machine is not essential, as the disposable credit cards or single use credit cards could be purchased in the normal way in which one purchases any other goods or services, such as either directly in a face-to-face transaction or by post.

Similarly, while in the above it has been suggested that there could be single use credit cards that would be purchased, there is no reason why they could not be multiple transaction credit cards with an aggregate credit limit. Further, these cards could, instead of being credit cards, be simply credit card numbers for single or multiple use. It is, however, envisaged that for operational efficiency, these numbers are much more likely to be issued as disposable credit cards or single use credit cards. Thus, for those who do not wish to handle a credit card or whose credit worthiness is such that they would not be allowed to have a credit card, it will now be possible for them to have the use of a credit card. This would have considerable advantages for the credit card providers.

In processing a transaction as described above, one step is to determine whether or not a limited use credit/debit/charge card number is valid. As discussed above, when a new credit card is presently issued, it is commonly required that the card holder activate the card. Specifically, the card holder may be required to communicate with the credit card issuer to activate the card before it can be used. Alternatively, in one embodiment of the present system, the card holder can control the activation or validity of a credit card number, or equivalent transaction code, during the course a transaction. Thus, in this embodiment, the card holder has the control, security and confidence that payments can only be made with his or her express permission.

Fig. 9 is a flow chart illustrating an exemplary method of controlling the validity of a limited use credit card number. The card holder has a credit card number, or equivalent transaction code, that is allocated to the card holder, but is not yet active. (Step 902). The card holder can acknowledge delivery of the credit card number, but the number remains inactive within the card issuer's processing system, e.g., a bank's processing system. (Step 904). When the card holder wishes to conduct a transaction, he or she contacts the card issuer to activate the credit card number. (Step 906). Activating the credit card number before every transaction is cumbersome, but in the context of a remote transaction for example, via the Internet or equivalent network, the communication between the card holder and the card issuer can be achieved very rapidly by an entirely automated system that will activate

the card during the process of conducting a transaction with an Internet based merchant. The credit card number is activated for a specific transaction only when specifically requested by the card holder. (Step 908).

The properties of this validation or activation process can vary. For example, the validation could be for a specific time period, for a specific merchant or group of merchants, for a specific type of transaction, or for a specific number of transactions (authorizations and/or presentments). These properties can also be combined in any permutation. For example, a card holder could request that his or her credit card number be validated for one transaction with a specific merchant up to a specific value limit or value range (e.g., a specific value +/- a configurable range). In the event that no authorization is received within a defined period, the validity can lapse. This combination provides a solution that meets the need for a secure, flexible payment system for remote transactions.

More specifically, for Internet transactions the card holder would receive a software package from the card issuer along with a unique personal validity limited credit card number. This software package would also facilitate completion of the merchants web page using ECML (electronic commerce modeling language) or some other equivalent electronic wallet system. Merchants wishing to use this system provide a unique merchant identification number on their web site. For merchants who are not compliant with such systems, a simpler automated method, e.g., "drag and drop," of transferring card number and other details is supported.

When a card holder wants to conduct a transaction, he or she activates the validity limited credit card software using a password or hardware based user identification system (e.g., magnetic stripe card reader, chip card reader, electronic token generator, fingerprint recognition system or the like) thereby identifying himself or herself with the card issuer. The card holder then requests his or her credit card number to be validated for the merchant as identified by the merchant identification number. After use the card number is automatically inactivated again. The card holder may also specify additional limitations as discussed above, such as value

limitations and maximum number of available transactions. Alternatively, these limitations could carry default limitations, for example single transactions up to a value of $100.00. This request would be transmitted via the Internet to the card issuer's card computer processing system. The processing system would validate the card holder's password (or hardware device), if appropriate, and forward the appropriate validity request to the card processing systems database.

The card issuer's server may also verify the merchant's identity by providing confirmation of the merchant's name as it will appear on the card holder's credit card statement. This merchant verification helps to avoid a common source of potential confusion for card holders in credit card transactions. The merchant identification number can either be the actual credit card systems merchant-ID or another unique code. In either case, the credit card merchant-ID that will be transmitted to the processing system during the transaction is entered into the processing system's database. This ensures that only the intended merchant can initiate a transaction with the validated credit card number. In the event that a merchant identification code does not satisfy the card holder's expectations, the card holder has the option to cancel the transaction before any information is passed to the merchant's web site.

When application of the one or more limitations are confirmed, generally within a matter of seconds, the card holder is given verification of such and is allowed to transfer the credit card number and transaction details to the merchant's web site. Since the merchant identification number is used to validate a specific number of transactions for that merchant, there is no benefit of a rogue or fraudulent merchant trying to steal the identity of another valid merchant. The transaction can only be reimbursed to the merchant identified to the card holder by the card issuer's system.

When a merchant receives the card holder's credit card number, the merchant processes this in an identical manner to an existing transaction in known systems. The transaction is passed through to the card issuer's processing system via the merchant acquiring and credit card networks. At the card issuer's processing system, the transaction is handled by an authorization system that allows a card number to

have associated validity restrictions or limitations, such as merchant-ID. If, in response to an authorization request, the authorization system indicates a valid card number, with an appropriate merchant-ID validation and sufficient funds, a normal authorization response is returned to the merchant. The number is then deactivated by the use triggered processing software within the authorization system or the in case of a multiple outstanding transactions the properties of the card number are updated to remove the permission for the authorized transaction (e.g. decrement the cumulated value limit). If the authorization system identifies a problem with the request, for example, exceeding a limitation, the merchant is denied authorization. Transaction settlements and card holder billing proceed as described above.

In the situation where a card holder is making multiple purchases with the same merchant within a short period of time, each validation by the card holder may be cumulative so that all the requested transactions can proceed. For example, if the card holder requests two transactions, one of $50.00 and one of $100.00 dollars for a specific merchant, the credit card number will be validated for two transactions to that merchant with a cumulative limit of $150. This means that both transactions will be authorized. In this case, the sequence of authorization requests from the merchant may differ from original sequence of validation requests from the card holder.

This system may be implemented using the internet card software package, or RAD software package, as described herein.

In general, the system provides a method for numbers and accounts to be set up and issued directly to the user. In addition, the system also permits users to directly alter the properties of a credit card account within an issuer's authorization and settlement system. The set-up (issuance) and use of a limited use credit card number can take place at the same time, i.e., in the same interaction or at separate times, i.e., setting up (issuing) a limited use credit card number at one time and configuring the limited use credit card number at a later time.

This system has a number of advantages over existing credit card systems. Card

fraud is greatly reduced since a stolen number requires the card holder to validate the card number before any transaction can be completed. This protects against either interception of the number during a transaction or the number being accessed from a merchant's computer systems at a later date. In addition, if the number is authorized, the merchant is assured that the card issuer has directly validated that the card holder has requested the transaction. This prevents or limits a card holder's ability to repudiate the transaction. Moreover, the card holder has additional control on the purchasing power of his or her credit card. The card holder has the reassurance that payment can only be made to the merchant described by the card issuing bank/organization.

In situations where the card-holder and card issuer are in communication and authentication is required of one or both parties, the list of limited use card numbers held by each party can used as a form of identification. In the manner of a dynamic password all or part of a single limited use number a sequence of such numbers could be used to identify either party without the need for issuing any additional security systems. Since this identification does not need to be handled by conventional transaction systems, all or part of a limited use number can be used for this purpose.

Fig. 10 is a flow chart illustrating an exemplary process for using a credit card number as a PIN number. In step 1002, a card issuer generates a database of available credit card numbers. The card issuer selects a master credit card number or more generically master account number (step 1004) and distributes the master account number to a master account number owner. (Step 1006). The card issuer then allocates additional credit card numbers to the master account number (step 1008), and distributes the additional credit numbers to the master account number owner. (Step 1010). When the master credit card number owner needs or desires to access account information (step 1012), the master account owner can use one of the additional credit card numbers as a PIN number. (Step 1014).

As can be readily seen, there are fundamental differences between the system of the present invention and any system that uses a PIN or other number (whether constant

or varying from transaction to transaction) to validate a transaction. In the present system the numerical details conveyed in the course of a transaction are identical in format to an existing credit card number but no unique account code is included. This maximizes the security and privacy of a credit/debit/charge card transaction. Within the processing system the validity of the limited use number is verified first and then the associated account identified second by examining information stored with the limited use number. With the transmission of an additional PIN or other number in addition to the account number or other unique identifier, there is a lower level of security and privacy. Within any form of PIN identification (and as described by Rahman) the associated account is identified first and then the PIN verified after this step. For this reason many card holders can share the same PIN, indeed in most cases due to the short length of PIN codes many users do have identical PINs but different account numbers. For our system each limited use number must be unique at the time of use and so the associated account can be uniquely identified.

With reference back to Fig. 1, and as described above, central processing system 100 can internally perform the approval and denial of credit card transactions or this function can be delegated to a separate clearance processing facility. In other words, central processing system can be located within the card issuer's main processing system or at a stand-alone facility. In an exemplary embodiment of the present invention, central processing system 100 adds additional functionality to existing credit/charge/debit card systems without any, or with minimal, alterations. In general, central processing system 100 transmits certain transaction details in a bi-directional manner, i.e., utilizing dual interfaces between central processing system 100 and the merchant and between central processing system 100 and the card issuer, without revealing the master credit card number to the merchant. The dual interface transmissions, referred to herein as remapping, allow merchants and card issuers to handle transaction details in the same manner as conventional credit card transactions. Such conventional credit card transactions may be, for example, authorizations, settlements, copy requests, and charge-backs.

Remapping can be implemented by utilizing database look-up functions using existing industry-standard computer platforms. In addition, remapping may occur by replacing the limited use card number with the master account number.

Fig. 11 is a block diagram illustrating a credit card system 1100 in which a central processing system 1106 in accordance with an embodiment of the present invention is located within a card issuing bank's main processing system 1114. System 1100 includes merchant acquirers 1102 connected to card issuing bank's main processing system 1114 via credit card network 1104 and switch 1116. Credit card network 1104 may be any type of communication network, such as the Internet, a radio network, etc. as described above. Switch 1116 includes hardware and software components. Switch 1116 may be configured to direct incoming transaction details on the basis of the card number and to direct outgoing transaction details on the basis of the merchant acquirer identification number (referred to herein as the "merchant ID").

Issuing bank's main processing system 1114 includes issuing bank processing facility 1112 and central processing system 1106. Central processing system 1106 includes acquirer interface 1108 and STIP interface 1110.

Exemplary transactions will now be described with reference to Figs. 11 and 12. Fig. 12 is a flow.chart illustrating an exemplary method of conducting a limited use credit card number transaction. A user initiates a transaction by presenting a limited use credit/charge/debit card number, either in person or remotely as discussed above. (Step 1202). Merchant acquirer 1102 routes this limited use credit card number to central processing system 1106 via network 1104 and switch 1116. (Step 1204). This routing is done on the basis of a specific bank identification number (referred to herein as "BIN") which is the first few digits of the limited use credit card number, as discussed above. In this example, central processing system 1106.acts as a stand-in processor.

If the limited use credit card number is invalid, or if the limited use condition has been satisfied, i.e., the condition has been met or exceeded, step 1206, central processing

system 1106 will transmit a signal to merchant acquirer 1102 denying authorization of the card number via switch 1116 and network 1104. (Step 1208). If the limited use credit card number is valid, and if the limited use condition has not been satisfied, central processing system 1106 transmits a signal to the issuing processing facility 1112 via merchant acquirer interface 1108 and switch 1116. (Step 1210). This signal includes the original transaction details but the card number and the merchant ID are remapped. This remapping provides the master credit card BIN number so the signal will be routed to processing facility 1112. This ensures that the authorization can be obtained against the master credit card and that any resulting authorization, or denial thereof, is returned to central processing system 1116, as this appears to processing facility 1112 to be the merchant. (Steps 1212 and 1214). The authorization, or denial of authorization, is the remapped within central processing system 1106 to the original limited use credit card number and merchant ID. (Step 1216). Central processing system 1106 then transmits a signal to merchant 1102 authorizing the limited use credit card number, or denying authorization as appropriate, along with the original transaction details via switch 1116 and network 1104. (Step 1218).

Fig. 13 is a flow chart illustrating an exemplary method of conducting a settlement transaction. In a settlement transaction, merchant 1102 transmits a signal to central processing system 1106 via network 1104 and switch 1116 according to the BIN of the limited use card number. (Step 1302). Central processing system 1106 remaps the limited use credit card number with the master credit card or account number, the merchant ID with a central processing system ID and the merchant text description with a central processing text description, step 1304, and transmits this remapped information to issuer processing facility 1112 via switch 1116, step 1306. Processing facility 1112 settles the transaction by payment, if appropriate, to central processing system 1106. (Step 1308). Central processing system 1106 then remaps the master credit card or account number back to the original limited use credit card number, the central processing ID back to the merchant ID and the central processing text description back to the merchant text description, step 1310, and transmits this information along with the payment, if appropriate, to merchant acquirer 1102 via switch 1116 and network 1104, step 1312. As with the authorization cycle, this

settlement cycle ensures that settlement is obtained against the master credit card; that the card holder's billing statement reflects the limited use transaction, with the central processing ID, and that the payment for settlement is conducted through central processing system 1106.

If a card holder challenges or questions a specific charge on his or her billing statement, the copy request or charge back will be routed to central processing system 1106, as this is the ID associated with the transaction. In a similar manner to that described above, central processing system 1106 will remap the copy request or charge back according to the merchant ID and the limited use credit card number and transmit the copy request or the charge back to merchant 1102 via switch 1116 and network 1104. Merchant 1102 transmits the requested copy or the charge back confirmation to central processing system 1106 via network 1104 and switch 1116 according to the BIN of the limited use card number. Central processing system 1106 then remaps the ID and card number information and forwards the requested copy or charge back information to processing facility 1112 via switch 1116.

System 1100 is advantageous in that it reduces communication delays and fees but it requires the addition of switch 1116. Alternatively, Fig. 14 illustrates central processing system 1406 as a stand alone facility. The authorization, settlement, copy request and charge back transactions described above are equally applicable to Fig. 14, except switch 1116 in Fig. 11 is no longer required. Fig. 14 illustrates that communication between central processing system 1406 and card issuing bank's processing facility 1412 can be conducted through existing credit networks 1404. In addition to not requiring a switch, such as switch 1116, in this configuration, a single large central processing system 1406 can offer limited use support to a wide range of issuers, such as bank processing facility 1412. However, this configuration requires increased communication times and potentially increased communication fees.

In another exemplary embodiment, the central processing system could be constructed to be a part of the merchant acquirer, instead of the bank processing

facility as shown in Fig. 11. This configuration would also require the addition of a switch like switch 1116 but would reduce communication delays and fees.

The limited use credit card number and remapping system may also be used in connection with organizations other than banks. For example, the limited use credit card number may be linked to organizations such as utilities, internet service providers, telephone accounts, fixed or mobile, anonymous prepaid accounts and the like. With such other organizations, there would be no remapping to a master credit card number, but rather to some other account number provided by the organization.

Linking a limited use credit card number to other organizations is advantageous for several reasons. First, the organization may have a pre-existing relationship with the user of the limited use credit card number. This relationship provides evidence of the user's credit history with the organization, so no additional credit checks need to be performed, which can be costly and time-consuming for the organization. In addition, because the organization is already providing other services to the user, a billing procedure is already established. The time and cost associated with establishing and implementing billing procedures has already been incurred. Minimal cost and effort is associated with adding a section to a billing statement for a limited use credit card number.

A card holder may desire to access a list of limited use credit/debit/charge card numbers where the limited use cards are not stored on the card holder's own computer. In the context of modern client server architecture this represents one extreme of the situation where all information storage is at the server. The previous description for local storage indicates the situation of a client program with a significant amount of local functionality. Between these two extremes a range of intermediary client server arrangements such as a "thin client" with minimal functionality obtaining limited use numbers from the server as required. The combination of encryption and dynamic passwords, as described herein, or any suitable alternative form of use identification allows a card holder to have "multiple

wallets", i.e., a card holder can access limited use numbers from different devices, without the need to transmit credit card numbers.

As discussed above, software and limited use numbers can be issued via electronic communication media. In one embodiment, a card holder can access limited use credit card numbers during electronic transactions via a Remote Access Device, referred to herein as "RAD", such as the Orbis Internet Card□. The overall layout of the RAD system 1500 is shown in Figure 15 and a flow chart illustrating an exemplary method of providing remote access devices for accessing limited use credit card numbers is shown in Fig. 16. In general, the operation of the complete system from registration to completion of a transaction follows.

When a user desires to register with RAD system 1500, the user submits user authentication information, the master account number and other identifying data for entry into a database 1502. (Step 1602). To register with RAD system 1500, the user must be a valid holder/user of the master credit card o r account number. (Step 1604). Once registered, step 1606, the user obtains a RAD 1504, step 1608. RAD 1504 includes a software package to which enables communication with a remote access device support server, referred to herein as a RAD support server 1506, such as the Nexus User Support Server□, to enable the issuance of limited use card numbers.

When the user initiates communication with RAD support server 1506, step 1610, RAD support server 1506 first authenticates the user, step 1612. If successfully authenticated, the user can then request a limited use number, step 1614 specifying any additional transaction limitations desired as discussed herein, step 1616. RAD support server 1506 issues a request over a network to a central processing station 1508 for a limited use number with the one or more specified limitations. The limited use number provided in response to the request is associated with a specific RAD system user identification previously assigned to the user.

Central processing station 1508 obtains the next available limited use number. (Step

1618). Once obtained, the limited use number, and the specified limitations, is entered into database 1502 such that the limited use number is associated with the user's information already in database 1502. (Step 1620). The limited use number is then transmitted to the RAD support server 1506 for issuance to the user via RAD 1504. (Step 1622). RAD software package 1504 displays the limited use number. The user can transfer this limited use number to a web site for initiating a transaction. Transferring this number to a web site can be achieved by dragging and dropping the number onto the web page, by software-simulated key-stroke entry, by "one-click" methods, or by other suitable methods known to one skilled in the art.

When a merchant 1510 receives a transaction utilizing a limited use number from RAD system 1506, the transaction details are handled in the same manner as an existing number since limited use card numbers share the same format as existing credit card numbers. The transaction details are transferred to the merchant acquirer and then routed onto the appropriate issuer on the basis of the leading digits of the limited use number, i.e., BIN, via central processing station 1508. The BIN is registered with central processing station 1508 to ensure appropriate routing.

As described above, central processing station 1508 verifies the validity of the limited use number and ensures that the transaction meets all specified limitations. If the limited use number is valid and the transaction met the specific limitations, central processing station 1508 enters the master credit card number into the transaction message in place of the limited use number. Central processing station 1508 then transmits the transaction message to the issuer's processing facility 1512 as a normal authorization request. The issuer's processing facility 1512 transmits an authorization for the master card number, if appropriate, to central processing facility 1508. Central processing facility remaps the master card number to the limited use number and the transaction message is transmitted to the originating merchant acquirer and then the merchant. Central processing station 1508 also updates the limitations and validity of the limited use number according to the details of the transaction. The limitation and validity updating is best done following verification of available funds so that a limited use number with a cumulative value limit is only decremented in value if the

transaction can be completed. If limitation and validity updating is done prior to checking for the availability/validity of the linked or principal account then certain updates will need to be reversed in the case of a decline on the linked or principal account. This has a small computational overhead. If the authorization was approved by the issuer's processing facility 1512, the user's purchase can proceed as normal. If declined, a decline message is sent to the merchant.

For settlements, the same routing occurs with all transactions deriving from a limited use number obtained from RAD system 1500.

The above described system will now be discussed in greater detail.

RAD system 1500 may be configured to provide the user with many features. RAD system 1500 enables the user to have multiple and different remote devices from which the user may access RAD support server 1506. In addition, it enables a user to have multiple credit card accounts with one or more issuers and to select from amount these multiple accounts. The RAD software package 1504 enables users to have additional passwords associated with an account if desired. The additional passwords can be used, for example, for children and can have additional pre-defined limitations such as a low dollar transaction limits, e.g., $50.00, or merchant class restrictions, e.g., gas stations.

The RAD software package 1504 includes a simple intuitive interface for the ease of the user, the appearance of which may be customizable without modification to the underlying code. RAD 1504 may use images that relate to the front and back of a credit card to provide key areas of functionality. The back of RAD 1504 includes an interactive panel with a magnetic stripe for providing additional information and/or advertising panels. The interactive panel/stripe area provides for password entry and functional selections. Upon activation, the front of RAD 1504 may be configured to provide additional functions, e.g., those required to initiate an on-line purchase. As discussed herein, supplying information required for on-line purchases can be automated in a number of ways including "clicking and transferring" the information,

"dragging and dropping" the information, or "one click shopping."

In one embodiment, RAD software package 1504 is configured to issue a sequence of paired numbers which are securely issued and activated and/or decrypted by oral or written authorization, such as the communication of a password. These paired numbers include an identifier code and a mask code. In order to retrieve a limited use number, a user at a remote device identifies himself or herself using his or her RAD software 1504 by transmitting the identifier code, such as a dynamic password to RAD support server 1506. RAD support server 1506 compares the identifier code with the particular RAD software package 1504 and accepts, or validates, the identifier code if appropriate. If valid, RAD support server 1506 determines the matching mask code for that identifier code from database 1502. RAD support server 1506 uses the mask code to encrypt the limited use card number as described above, and transmits this encrypted code to the user. RAD software 1504 decrypts the encrypted code using the known mask code and reconstructs the initial digits, the BIN number and the checksum digit. RAD software 1504 then arranges this information and reconstructs the limited use card number.

RAD support server 1506 is an Internet based server that interfaces the RAD 1504 and central processing station 1508. RAD support server 1506 receives requests for limited use numbers from users, validates each user, if appropriate, and supplies and validates limited use card numbers with specific limitations, as requested by each user, if appropriate. Such requests may be processed in any desired order, e.g., first come first served basis. RAD support server 1506 may also be configured to provide for location identification verification, secure delivery of limited use numbers, automated completion of payment fields in a merchant's web page order form, review of previous transactions, access to additional issuer services and advertising. The RAD location identification verification is verifying the physical source of the request for a limited use number, e.g., home, office, ATM machine. This additional identification is evidence to limit a user's ability to deny a transaction. The RAD support server 1508 can be configured to require additional identification of the user if the RAD is being used from a physical source which is unknown to the RAD support

server or which has not been previously associated with the RAD by the user.

To accomplish the above tasks, RAD support server 1506 should have a high bandwidth Internet connection and highly secure firewalls to insulate critical information from undesired access. Communications between RAD support server 1506 and RAD 1504 is may be Internet based. Communication between RAD support server 1506 and central processing station 1508 and database 1502 may be secured via private networks for additional security. In addition, to provide for additional security, RAD support server 1506, central processing station 1508 and database 1502 may be located at the same physical location, for example, the issuer's processing facility or some other facility which meets the standards set for banking processing facilities.

Communication between RAD 1504 and RAD support server 1506 can use industry standard security protocols appropriate to the platform. For example, secure socket layer (SSL) encryption may be used in the case of communication by a personal computer of the Internet. Alternatively, one of the encryption schemes described herein may be implemented alone or in combination with password protection and/or smart card user authentication. Such communication security can be selectable by the issuer. For example, issuers can select what type of communication security they desire from a range of options.

While the foregoing description makes reference to particular illustrative embodiments, these examples should not be construed as limitations. Not only can the inventive system be modified for other card numbered systems; it can also be modified for other computer networks or numbering schemes. Thus, the present invention is not limited to the disclosed embodiments, but is to be accorded the widest scope consistent with the claims below.

CLAIMS

1. A method of controlling the validity of a limited use credit card number in a financial transaction system capable of using at least one limited use credit card number which is deactivated upon a use-triggered condition which occurs subsequent to assignment of the at least one limited use credit card number and which is associated the master account number of a customer comprising the steps of:

sending to a customer from a limited use credit card number issuer a limited use credit card number which is not yet activated;

receiving acknowledgment of delivery by the customer of the limited use credit card number which is not yet activated;

communicating with a limited use card number card issuer to activate the limited use credit card number before it can be used in a transaction; and

validating the limited use credit card number to have associated limited use properties.

2. The method of claim 1 wherein said limited use properties are one or more properties selected from a group consisting of: a specific time period, a specific merchant, a specific group of merchants, a specific type of transaction, and a specific number of transactions.

3. The method of claim 1 or 2 wherein said sending step includes sending to the customer a software package from the card issuer along with a unique personal validity limited credit card number, said software package facilitating completion of the merchants web page.

4. The method of any preceding claim wherein said validation step includes:

activating validity limited credit card software using a user identification to identify the user with the card issuer;

requesting validation of a limited use credit card for a merchant as identified by a merchant identification number; and

providing an opinion for a user to specify additional limitations other than the specific merchant to the limitation on the limited use credit card number.

5. The method as claimed in any preceding claim further comprising the steps of:

receiving by a merchant a limited use credit card number;

processing by a merchant the received limited use credit card number in a transaction as any other credit card number;

passing the transaction through to the card issuer's processing system;

requesting authorization of the transaction at the card issuer's processing system against the associated limited use properties; and

deactivating the limited use credit card number by the card issuer when a use-triggered condition is present.

6. The method as claimed in any preceding claim further comprising the steps of:

deactivating the limited use credit card number by the card issuer when a use-triggered condition is present;

communicating with the card issuer to reactivate the limited use credit card number to be used in one or more additional transactions subsequent to the deactivating step; and

revalidating the limited use credit card number with associated limited use properties.

7. The method as claimed in any preceding claim wherein the limited use properties of the revalidated limited use credit card number are different from the limited use properties of the validated limited use credit card number.

8. A method of conducting a limited use credit card transaction in a financial transaction system capable of using at least one limited use credit card number which is deactivated upon a use-triggered condition which occurs subsequent to assignment of the at least one credit card number comprising the steps of:

initiating a transaction by a customer presenting a limited use credit card number to a merchant;

routing said limited use credit card number to a central processing system; and

determining whether said limited use credit card number has been deactivated because at least one use-triggered condition has been satisfied.

9. The method of claim 8, wherein the limited credit card number is linked to an organization selected from a group consisting of: a utility, a public network service provider, a telephone company, a bank account, a prepaid account and a credit card issuer.

10. The method of claim 8 or 9 further comprising